Windows 2003 Server

Course Outline

MSTP

- WINDOWS 2003 PRODUCT LINE
- PLANNING
  - Installation methods
  - Hardware Requirements
  - NTFS/RAID
  - Workgroup v.s. Domain
- USER MANAGMENT
  - The MMC
  - User Account
- GROUPS
  - Types
  - Creating
- GPO’s
- SERVICES
- DISASTER RECOVERY

WINDOWS 2003 PRODUCTS

W2K3 Basics

MSTP

- The Windows Server Family
- Windows Architecture
- Underlying Technologies
- Review
- Quiz Yourself

W2K3 Product Line

MSTP

- Windows Server 2003—Standard Edition
- Windows Server 2003—Web Edition
- Windows Server 2003—Enterprise Edition
- Windows Server 2003—DataCenter Edition

W2K3—Standard Edition

MSTP

Windows Server 2003 has the following limitations:

- A maximum of four microprocessors may be used.
- No more than 4GB of memory is allowed. Of that 4GB, the operating system always reserves 2GB for its own use, allowing applications on the server to share the remaining 2GB.

W2K3—Web Edition

MSTP

The Web Server edition is optimized for Microsoft's Internet Information Services (IIS) Web server platform. The Web Server edition does not support some advanced services, including:

- Advanced network security features like Internet Authorization Server
- Fax services
- Terminal services

W2K3—Enterprise Edition

MSTP

It provides all of the same features and capabilities as the standard edition and adds the following:

- Support for up to eight microprocessors in a server.
- Expanded memory support that reserves only 1GB of memory for the operating system, allowing applications on the server to share the remaining 3GB.
- The ability to create clusters of two servers.

W2K3—Datacenter Edition

MSTP

Like the Enterprise Server edition, Datacenter Server builds upon the standard Windows Server 2003 edition and adds the following features and capabilities:

- Support for up to 32 processors in a single server
- Support for up to 64GB of memory
- Support for clusters of up to four servers

Windows Architecture

MSTP

- Windows Server 2003 is a multithreaded, multiprocessing, multitasking operating system.
- Windows Server 2003 also offers compatibility with an enormous array of hardware devices, allowing the operating system to interact with storage devices, scanners, networks, and many other types of peripherals.

Review

MSTP

In this session, you learned about the four editions of the Windows Server 2003 family:

- Windows Server 2003—Standard Edition
- Windows Server 2003—Web Edition
- Windows Server 2003—Enterprise Edition
- Windows Server 2003—Datacenter Edition

You also learned about Windows' operating system and application architecture, including Windows' ability to perform multiprocessing, multitasking, and multithreading.

Finally, you learned about many of the basic technologies that Windows is built on, including TCP/IP, Windows' security model, and its graphical user interface, or GUI.

QUIZ YOURSELF

MSTP

1. Which edition of Windows Server 2003 introduces the ability to create server clusters?
2. What is the main reason Datacenter Server is the most reliable edition of Windows Server 2003?
3. What part of Windows decides which tasks and threads are executed by the computer's processors?
4. What is the native networking protocol for Windows Server 2003?

PLANNING

Installing W2K3

MSTP

- Installation Methods
- Performing an Installation
- Upgrading from Prior Versions of Windows
- Product Activation
- Review
- Quiz Yourself

Installation Methods

MSTP

Windows Server 2003 offers three basic types of installation:

- A standard CD-based installation enables you to install the operating system from a CD-ROM drive, or even from a DVD-ROM drive, if you have one.
- A network-based installation doesn't require you to have a CD-ROM drive. Instead, the installation is run from a copy of the installation CD, which is located on a networked file server.
- A RIS-based installation uses Remote Installation Services, or RIS, to install the operating system without using a CD or a copy of a CD.

Install 2003 Server Preparation

MSTP

- **Check Hardware Compatibility List (HCL)**
  - One or more processors with a recommended minimum speed of 550 MHz (minimum supported speed is 133 MHz).
  - A maximum of four processors per computer is supported. Processors from the Intel Pentium/Celeron family, AMD K6/Athlon/Duron family, or compatible processors are recommended.
  - **256 megabytes (MB)** of RAM recommended minimum (128 MB minimum supported; 4 gigabytes (GB) maximum).
  - A hard disk partition or volume with enough free space to accommodate the setup process. To ensure that you have flexibility in your later use of the operating system, it is recommended that you allow considerably more space than the minimum required for running Setup, which is approximately 1.25 GB to 2 GB. partition **(NTFS is the recommended file system).**
  - VGA or higher-resolution monitor (Super VGA 800x600 or higher recommended), keyboard, and
  - **(optionally)** a mouse or other pointing device.

Upgrading from Prior Versions of Windows

MSTP

- Windows Server 2003 can perform an upgrade if your computer is already running:
  - Windows NT Server 3.51,
  - Windows NT Server 4.0, or
  - Windows 2000 Server
- cannot perform an upgrade on a computer running:
  - Windows 9x,
  - Windows NT Workstation, or
  - Windows 2003 Professional.

Product Activation

MSTP

- Product activation is tied to the product ID number you provide to the Setup Wizard when you install Windows Server 2003.
- Product Activation Compared to Product Registration
  - product activation is required
  - Product registration is completely optional
    - All registration information provided is stored securely

What licensing mode to use

MSTP

With products in the Windows Server 2003 family, you can choose between two licensing modes:

- **Per Device or Per User**
  - Per Device or Per User mode requires a separate Client Access License (CAL) for each device or user that accesses a server running a product in the Windows Server 2003 family.
  - Per Seat/User more economical for large organizations
    - This is what USMC uses. Each Computer connecting has a license
- **Per Server**
  - Per Server mode requires a separate CAL for each concurrent connection to a server.

REVIEW

MSTP

In this session, you learned about the various installation methods supported by

- Windows Server 2003:
- CD-based
- Network-based
- RIS-based

You also learned about attended and unattended installations, how to create answer files for unattended installations, and how to start both attended and unattended installations. You learned about Windows Server 2003's ability to upgrade your computers' existing operating systems, and you learned about the product activation required by Windows Server 2003. Finally, you learned about Windows Server 2003's new "headless server" installation capabilities.

QUIZ YOURSELF

MSTP

1. What are the three ways you can install Windows Server 2003?
2. How do you initiate a CD-based installation? (See “CD-based installation.”)
3. What two commands can be used to initiate a network-based installation?
4. What special type of network interface card (NIC) is required to perform an installation using RIS?
5. What are two ways to create an answer file for use in an unattended installation?
6. What operating systems can be upgraded to Windows Server 2003?

File and Partition Sizes

MSTP

- NTFS can store up to 16 exabytes in size.
  - Exabyte =1,000,000GB -Terabyte =1,000GB
- Minimum partition size for NTFS is 50MB.
- Anything smaller – FAT recommended
- NTFS takes nearly 25% of the partition’s total space for directory overhead, whereas FAT takes almost none.
- You can reclaim the space taken by NTFS by setting compression on the entire volume, this is not available on FAT.

NTFS Fault Tolerance

MSTP

- NTFS logs all changes to the file system, which means it can redo or undo every file or directory update to correct discrepancies arising from system failures or power losses.
- Uses a method called *hot fixing* repair disk failures on the fly; hot fixing does not return an error message to the calling application.
- After every write to a hard disk, the sector is reread to verify it's integrity.
  - *If data is different, the sector is flagged bad and the write is preformed again to a different place.*

Domain Controller Setup

MSTP

- No need to promote or demote a domain controller
- Add additional domain controllers for redundancy and reduce the load on existing domain controllers
- To install 2003 Server execute command **dcpromo**
- If create first DC in domain, creating either a new child domain, or new domain tree

Network Setup

MSTP

- If this is the first computer in the domain network setup will have to wait until your services are configured
- Joining an existing domain as a member server is the same as joining an NT domain

DCPROMO

MSTP

- Makes 2003 Server a domain controller
- Run after reboot server installation
  - O/S is 2003 Server, Standard Edition or Enterprise
  - TCP/IP must be installed
  - Network connectivity must exist
  - The correct time and zone must be specified
  - DNS server available on the network
    - If not, DCPROMO will create this server as one
  - One NTFS volume is required for Active Directory
  - User with administrative rights

USER MANAGEMENT

Managing Users and Groups

MSTP

- Server Security
- Local Users and Groups
  - Users
    - Managing users
    - Built-in users
  - Groups
    - What groups should you create
    - Managing groups
    - Built-in groups
- Local Account Policies
  - Password polices
  - Account Lockout policies
- Security Auditing
- Review
- Quiz Yourself

Planning User Accounts

MSTP

- Naming conventions must be consistent and uniquely identify users to the domain
- Use unique logon, max of 20 characters
- Logon names are not case sensitive
- Invalid characters – / \ [ ] : ; | = , + * ? < >
- Name space designations appended to logon
  - SMITHCA = smithjj@mstp.quantico.usmc.mil
- Passwords assigned, hard to guess and no longer than 128 characters (8 recommended)
  - Passwords can contain spaces, a good method for creating passwords is to use a phrase or sentence "I love Windows 2003 server"

Workgroup

MSTP

- Logical grouping of computers and users that share resources
- Each 2003 computer maintains a local directory database with its own accounts, administration, and security policies
- Similar to a peer-to-peer network
- Decentralized management
- Resources password protected, but must know
- Professional workstation or stand-alone server

Workgroup Advantages

MSTP

- Does not require a central server for administration
- Simple to design and implement
- Convenient for a limited number of computers, normally 10 or less
- Good for small amount of technical users
- Disadvantages?

Server Security

MSTP

Windows Server 2003 can play different roles on a network, depending on your security requirements:

- As a ***standalone server***, Windows Server 2003 maintains its own user accounts and groups.
- As a ***domain controller***, Windows Server 2003 maintains user accounts and groups that can be shared with other servers.
- As a ***member server***, Windows Server 2003 maintains its own user accounts, just like a standalone server.

Local Users and Groups

MSTP

A *user*, or *user account*, represents a real person who needs to use the resources on a server.

- ***Users***
  - User accounts are configured with several pieces of information:
    - A user name, or user ID, which uniquely represents and identifies the account—for example, “JoeL,” “Djonw,” or “RrondA.”
    - A proper name, which is the user’s full name.
    - A password, which is a series of numbers, symbols, and letters.
    - Account properties, which define special information about the user.

Cont.

MSTP

The Audit policies include:

- **Audit logon events.** This policy tells Windows Server 2003 to create Security Event Log entries whenever someone attempts to access the server.
- **Audit account management.** This policy audits the creation, modification, or deletion of user and group accounts.
- **Audit object access.** This policy allows Windows Server 2003 to audit file and folder access, helping to keep track of what files and folders are being accessed by users.
- **Audit policy change.** This policy audits any changes to the local security policies, so you can see if another user has changed the policies you have defined.

Old Server Manager Tasks

MSTP

- Shared Folders snap-in via an MMC
  - Remote management of shared folders
  - Remote viewing of which users are accessing shared resources
  - Remote disconnection of users from shared resources on a 2003 computer
  - Send a message
- Services snap-in via an MMC
  - Remote starting and stopping of services
- Specify remote computer when creating custom MMC

Old Server Manager Tasks

MSTP

- Add/remove computer from domain
  - During installation of 2003 O/S
  - To join domain, computer account must be created in or added to domain either during install or in advance (AD Users & Computers)
    - Users w/ Join A Computer to the Domain user right
    - Members of Administrators, Domain Administrators, or Account Operators
  - DC & DNS must be online when installing
- Join domain by using Network Identification tab in System Properties

Administrative Tasks

MSTP

- Highlight name; Use Action menu to select
- Disable don’t need account, but will use again
- Rename retain all rights, permissions, group memberships, & most properties to reassign
- Delete account is no longer used
- Resetting passwords entering new password
  - Do NOT need to know the old password
- Unlocking accounts violating policy

Group Types

MSTP

- Use AD Users and Computers to create
- Groups – collections of user accounts to ease of administration when assigning permissions (Security) or functions unrelated to security (Distribution)
- Security groups have capabilities of a distribution group included

Group Scopes

MSTP

- Domain local group (like NT)
- Global groups (like NT)
- Universal groups: Access resource any domain
  - Native mode only (only 2003 O/S in domain)
- Some local, global and universal groups created by default
  - Administrators, Users, Domain Admins, Domain Users, and Enterprise Admins
  - Can NOT rename default groups
  - Can NOT delete any built-in or system groups

Domain Local Groups

MSTP

- Purpose -- to control access to resources by assigning permissions within one domain
- Created on 2003 computers part of a domain and stored in domain directory database (SAM) on DC on which created
- If create a local group in CSS domain, maintained in directory database for CSS
- Non-domain local groups created on Professional/Stand-alone servers & apply to that computer

Permissions and Membership

MSTP

- Domain Local groups on 2003 servers DCs can be assigned permissions on any resource on any domain controller
- Permissions assigned to resources on stand-alone servers, member servers or workstation only apply to those machines
- Membership in domain local groups can include members from any domain in the tree/forest

Global Groups

MSTP

- To organize users performing similar tasks or network access requirements
- Only be created on domain controllers
- Assign permissions to gain access to resources that are located in any domain
- Membership only includes users from the domain in which you created the global group
- Users from other domains can not be placed in another domain’s global group

Global Group Nesting

MSTP

- Global group nesting is permitted meaning global groups can be put into other global groups to create a hierarchy of groups
- Unlimited levels of nesting ONLY in Native mode of 2003
- Nesting reduces network traffic between domains
- Nesting simplifies administration in a domain tree

Universal Groups

MSTP

- Used to assign permissions/give access to related resources in multiple domains
- Available in Native mode only
- Membership is members from any domain
- Use when membership is static since changes will be replicated increasing network traffic
- Add global to universal groups, assign permissions for resources to universal

Rules to Dealing With Groups

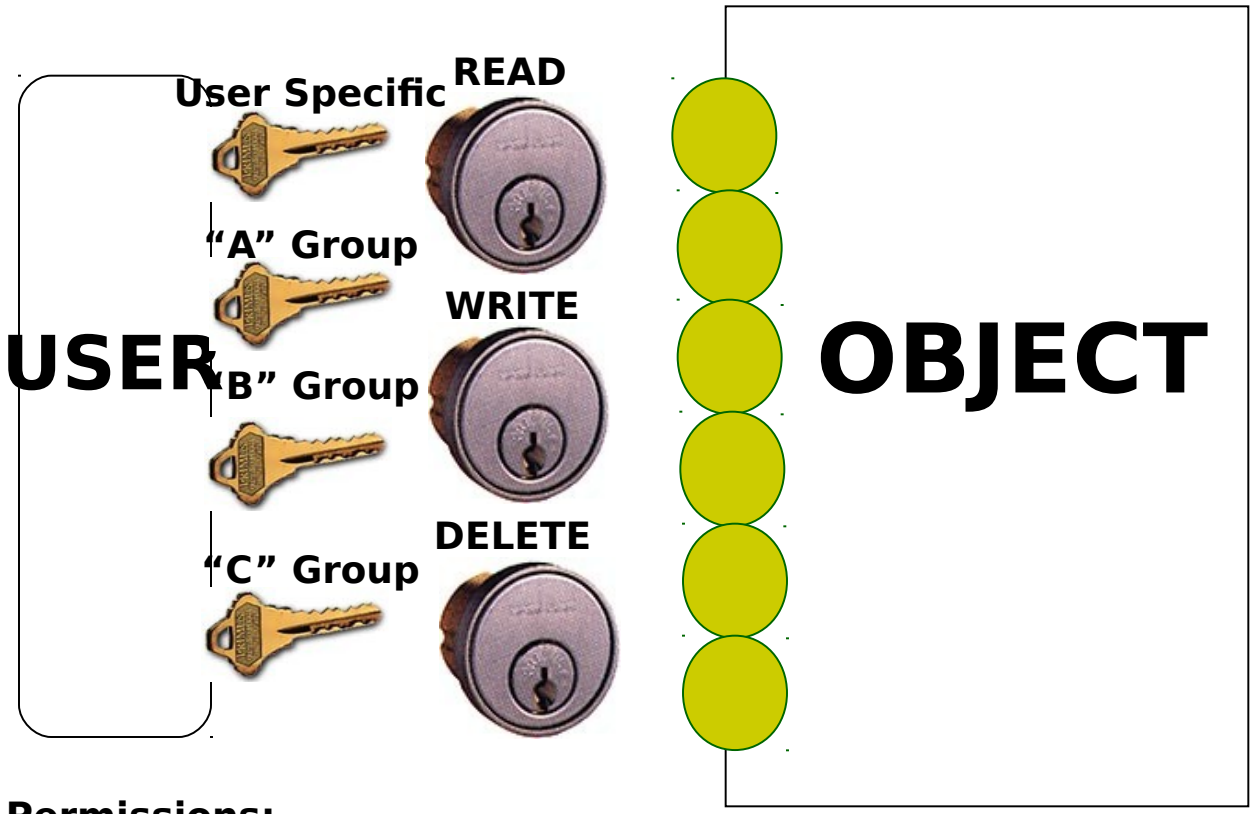
MSTP

- Prescribed method of applying permissions
- U-GG-DL(UG)-Permissions
  - Users go into global groups
  - Global groups are put into domain local groups or universal groups
  - Domain local groups or universal groups are given the permissions

Access Tokens and ACL's

MSTP

ACCESS TOKEN **ACCESS CONTROL LIST**

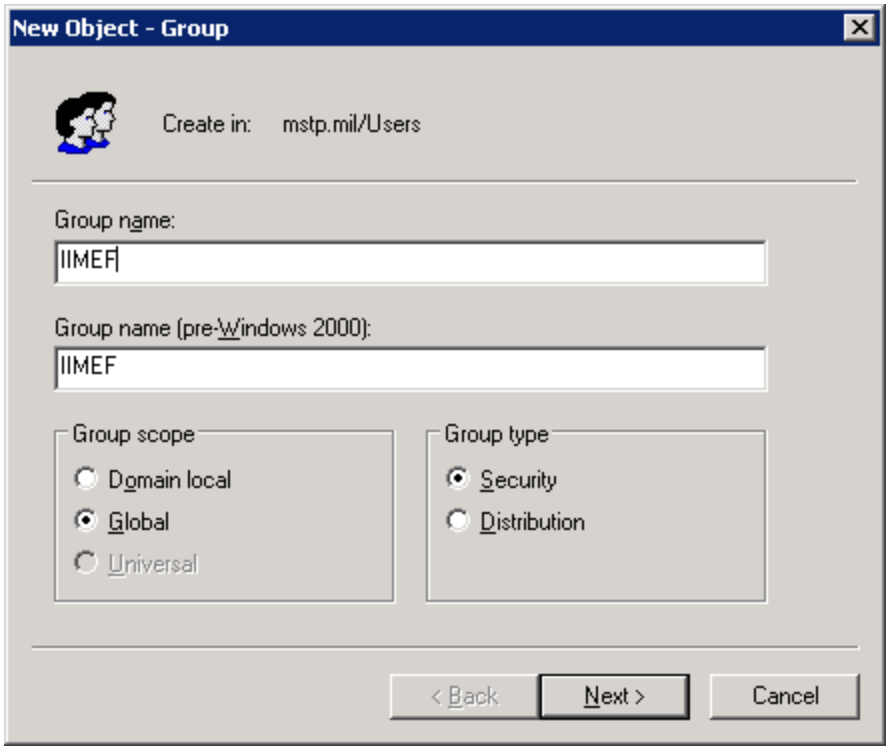


Permissions:
Share – responsible for controlling remote access to local resources. A share is a network resource: it is an object in itself which points to the resource object.
NTFS – Affect both local and remote access to a given object.

Creating Groups

MSTP

- Use AD Users and Computers
- Create in USERS container or OU
- Action Menu, New/Group
- In New Object – Group dialog box
  - Group name pertinent to asset/resource
    - **Note there is no different in icons to distinguish between local or global groups (only group/user)**
  - Group name for pre-2000
  - Group scope
  - Group type
- Users can't be added until group is created



REVIEW

MSTP

Windows Server 2003 has a very flexible security architecture. In this session, you learned how Windows Server 2003 can play different roles on a network:

- Standalone server
- Domain controller
- Member server

You also learned that standalone servers and member servers can have their own user and group accounts and that those servers come with several accounts built right in. You learned how to create your own users and groups, and you learned how to control user accounts by defining a server's local account policies. Finally, you learned how to use security auditing to keep tabs on how your servers are being used and by whom.

QUIZ YOURSELF

MSTP

- **1.** What are the names of the built-in Windows Server 2003 user groups?
- **2.** What are the names of the built-in Windows Server 2003 users?
- **3.** How can you control the minimum length of passwords used by local users?
- **4.** How do you enable security auditing in Windows Server 2003?

GPO's

Group Policy (GP)

MSTP

- Configuration settings that apply to one or more objects in AD
- Controls work environments for users
- Provisions
  - Auto delivery of applications to user for install
  - Delivers file/shortcuts to network/computer
  - Auto execution of tasks at designated times
  - Security settings for Account Policy, User Rights, Audit Policies, Event log, etc
  - Redirects folders to network locations

Group Policy Object Administration

MSTP

- The Group Policy snap-in is GPO-specific
- This allows user to add a snap-in for each GPO that you want to administer for a site, domain or OU where the GPO is located
- 2003 registry settings cleaned and rewritten each time policy changes in difference to NT which had to be explicitly reversed
- Reapplied every 90 minutes by default

Group Policy Application

MSTP

- Not part of domain -- local computer policy only
- Part of domain applied in a specific order
  - Windows NT policies from NETLOGON share
  - Local computer policy
  - SITE level policies
  - DOMAIN level policies
  - OU level policies
  - Child OU policies
- Exception -- account policies only at DOMAIN

Group Policy Association

MSTP

- Multiple containers in AD can be associated with same GPO
- Single AD container can have more than one GPO
- The scope of the GPO depends on the membership in security groups

Group Policy Sections

MSTP

- Computer Configuration (CC)
  - Customize user's environment & enforce lockdown policies for computers
  - Policies applied when the O/S initializes
  - Apply to every user logging on a computer regardless of the OU the user belongs
- Sub sections include Software Settings, Windows Settings, and Administrative Templates

Group Policy Sections

MSTP

- User Configuration (UC)
  - Customize the user's environment
  - Enforce lockdown policies for users
  - Include desktop appearance, application settings, logon and logoff scripts, and assigned and published applications
  - Apply when the user logs on to the computer
- Sub sections include Software Settings, Windows Settings, and Administrative Templates

Software Settings

MSTP

- Affects applications to which users can gain access
- Installations automatic by
  - Application assignment (upon connection the application will install automatically)
    - Computer Configuration Section
  - Application published (user has to use Add/Remove Programs to load the application) or assigned (application automatically installed)
    - User Configuration Section

Windows Settings -- Scripts

MSTP

- Allows scripts and batch files to be run at specified times
  - startup or shutdown (Computer Configuration Section)
  - log on/off (User Configuration Section)
- Automating of repetitive tasks
- Order of Execution
  - Startup, log on, log off, shutdown

NT vs 2003 Policies

MSTP

- Group policies created in Windows 2003 can NOT be applied to Windows 95/98/NT
- System Policy Editor policies can NOT be applied to Windows 2003
- If policy needs set for Windows 95/98/NT in a 2003 arena, use POLEDIT.EXE to create, but store CONFIG.POL or NTCONFIG.POL in the NETLOGON share for 2003 located in %systemroot%\SYSVOL\Sysvol*DomainName.com*\Scripts

Managing Group Policy

MSTP

- For domain or OU, use AD Users and Computers
- For site use AD Sites and Services
- Through either snap-in process is same
- For the Future
  - When and if XP clients start to come online, extended GPO options for Windows XP can be installed into the default Windows 2003 GPO options. See technet or search google.com for more information.

GPO Permissions

MSTP

- Default groups added to object
- Groups configured with a set of permissions
- Domain Admins, Enterprise Admins, System
  - Read, Write, Create All Child Objects, Delete All Child Objects, Edit of the GPO
- Authenticated Users
  - Read, Apply Group Policy (AGP)
- Creator Owner
  - Special Object and Attribute permissions assigned to child objects and properties within the GPO, Edit of the GPO

Deny

MSTP

- Policy settings do not apply to group members that have been denied Apply Group Policy permission (Deny)
- Administrators are part of the Authenticated Users group
- If don’t want policy to apply to administrators, deny or remove Authenticated Users group from the default settings

Policy Inheritance

MSTP

- GPs are passed from parent to child containers
- If assigned GP to a high-level parent container, that GP applies to all containers beneath the parent container including the user and computer objects in each container
- For instance, Group Policy set on the Domain level will flow down to the OU level

Policy Inheritance Concepts

MSTP

- If the child container has been explicitly defined a GPO it overrides the parent policy
- If a parent OU has policy settings not configured, they are not inherited
- Disabled settings are inherited as disabled
- If a policy is configured for the parent OU and a policy is configured for a child OU and they are compatible (no conflicts), child inherits the parent policy and child is also applied

Policy Inheritance Exceptions

MSTP

- If incompatible or the policies conflict, the child settings only apply to the child container/object.

Blocking

MSTP

- Administrator’s can configure inheritance
- Inheritance blocked for all policies from the levels above
- Performed at the domain or OU levels, not at the site level since top of hierarchy
- If multiple policies exist on the domain, NONE of the policies will filter to the OU that you have specified to block inheritance

Deleting Policy

MSTP

- DEFAULT DOMAIN POLICY GPO can NOT be deleted by an administrator
- Default Domain Policy contains required settings for the domain
- Can’t delete, but can disable the Computer and User configuration settings check boxes in the properties
- Can block inheritance if no override is not configured on the parent container

Disks, Partitions, and Drives

MSTP

- All new disks are referred to as *basic disks:*
  - cannot be used for special features like fault tolerance
- *logical drives*
  - they are assigned drive letters by the operating system
  - Drive letters A and B are reserved for the first two floppy disk drives
  - first hard drive partition is usually lettered C, the next one D

Disk Management

MSTP

You can use Disk Management to accomplish several important tasks:

- To create a new partition, right-click the empty area of a hard disk and select Create Partition from the pop-up menu.
- To change the drive letter assigned to a CD-ROM or partition, right-click it and select Drive Letters from the pop-up menu.
- To convert a basic disk to a *dynamic disk,* which supports more partitions as well as special features like fault tolerance, right-click the disk and select Convert to Dynamic Disk from the pop-up menu.
- To remove a partition, right-click it and select Delete from the pop-up menu.

Fault Tolerance

MSTP

- Windows Server 2003 helps prevent such losses by providing two levels of software-based fault tolerance: mirroring and RAID 5.

Mirroring

MSTP

- Mirroring allows two identically sized partitions, located on separate disks, to automatically duplicate one another.
- Both partitions become a *mirror set,* which means they always contain the same content and appear to the operating system as if they were a single partition.
  - Mirror sets use only one drive letter
  - Disk Management gives you the tools necessary to work with mirror sets:

RAID 5

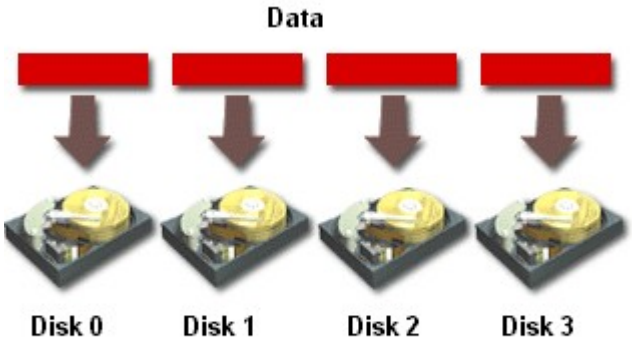
MSTP

- **RAID is an acronym that stands for *Redundant Array of Inexpensive Devices.***
  - can help improve fault tolerance
  - **speed up the process of reading**

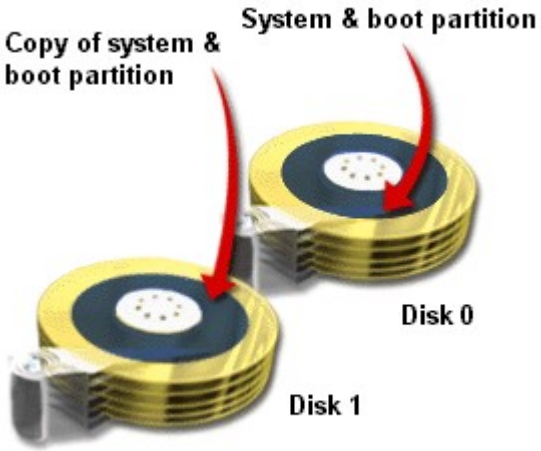
- **RAID 5 arrays consist of at least three partitions of equal size:**
  - RAID 5 volumes can be created only by using identically sized empty areas of dynamic disks.
  - The operating system saves data to all of the array partitions at once dividing saved information between them
  - The operating system calculates *checksum data.*
  - If one disk in a RAID 5 array fails, the checksum data from the remaining drives is used to recreate the data that was stored on the failed disk.
  - If two or more disks in the array fail, then all of the data on the array is lost.

Raid

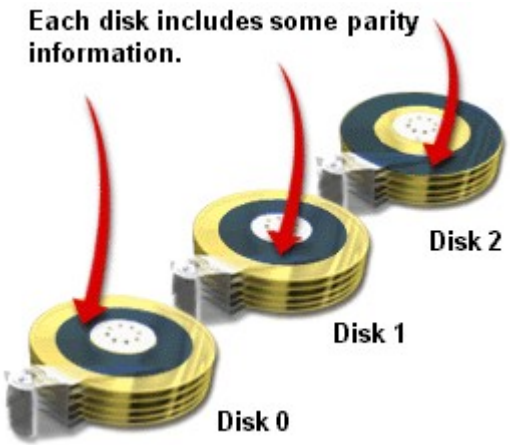
MSTP



Raid Level 1 - Mirror



Raid Level 5 – Stripe Set with Parity



REVIEW

MSTP

You learned about Windows Server 2003's organization of the disks in your computer, including basic disks and dynamic disks. You learned how to create partitions on a disk, select a file system for the partition, format the partition, and assign a drive letter to the partition. You also learned about Windows Server 2003's software fault tolerance features, including the ability to create mirror sets and RAID 5 arrays by using the Disk Management application. Finally, you learned some tips for optimizing the disks in your computer, such as striped sets.

QUIZ YOURSELF

MSTP

1. What kinds of disk fault tolerance does Windows Server 2003 offer?
2. What three main file systems does Windows Server 2003 support?
3. What are the advantages of the NTFS file system?
4. How can you change the drive letter associated with a specific partition?
5. When a new drive is added to a computer, what type of disk does Windows Server 2003 configure it as?

File Compression

MSTP

- Windows Server 2003 has the ability to compress files stored on any NTFS volume.
  - When compression is used, files take up less space on disk.
  - The operating system automatically decompresses files that are being accessed, so client computers don’t need to have any special compression software installed.
  - The operating system also recompresses files that are changed and then saved, ensuring that the file uses as little disk space as possible.

Performance impact of compression

MSTP

- Windows Server 2003 requires extra time when a user accesses a compressed file
- The operating system has to decompress (and recompress, if the file is changed and then saved) the file
  - The performance impact decompress a single file is very small
  - large number of compressed files, the additional work performed by the server becomes quite noticeable and can make the server seem unusually slow to respond.
    - Compression is most commonly used on files that are not used very often.

Compression

MSTP

Other files that might be eligible for compression include:

- Last year's accounting files, which aren't regularly needed but still must be available at a moment's notice.
- Old customer files, which might be needed in an emergency but are otherwise seldom used.
- Other archived data, which is accessed often enough to keep it on the server, but usually less than once or twice a week.

File Encryption

MSTP

- Windows Server 2003 provides the Encrypting File System (EFS).
  - EFS uses digital encryption keys to encode files so that only the owner, and users the owner designates, can access the files.

Performance of encryption

MSTP

- Similar to the extra time required for file compression,
  - Windows Server 2003 requires extra time to encrypt and decrypt files.
  - If a large number of users attempt to access a large number of encrypted files, the server may seem slow to respond.
    - Generally, only especially sensitive files are encrypted, so the negative performance impact of encryption is minimal.
- minimize the performance overhead of encryption is to encrypt only individual files.

Encryption

- When you encrypt a folder, Windows Server 2003 automatically encrypts the files within that folder, as well as any new files added to the folder.
  - The folder itself isn’t encrypted; it is simply marked so that future files placed within it will be automatically encrypted.

Rules for encrypted files and folders

MSTP

Encryption follows the same rules for moving and copying as file compression

- Encrypted items that are moved on the same volume retain their encryption;
- items moved to a different volume, or copied, take on the encryption attribute of their new folder.
- Remember that only the user who encrypts a file (or users they permit) can decrypt it.

Recovering encrypted files

MSTP

- Domain administrators define recovery agents using domain security policy.
  - “recovery agents”
    - The agents can decrypt any encrypted file.
  - To do so, they must back up the encrypted file,
    - restore it to a secure computer,
    - log on as a recovery agent, and decrypt the file

Disk Quotas

MSTP

- One of the most common uses for Windows Server 2003 is as a file server:
  - a central repository where users can store their data files.
- Disk quotas were created to help manage how users utilize server disk space.
  - Quotas assign specific space limitations (called *thresholds*) to specific users.
    - The thresholds apply for an entire volume, and users who exceed the threshold can be cut off—preventing them from using any more disk space.

Disk quotas and compression

- What if your users compress some of their files?
  - Windows Server 2003 uses the *uncompressed* file size in quota calculations, regardless of how much disk space the file is actually using.

REVIEW

MSTP

You learned how to use file compression to compress files so that they use less disk space than they normally would. You also learned how to use file encryption to protect sensitive files and how to recover encrypted data if necessary. You also learned how to use disk quotas to limit the amount of disk space users can fill up on your servers.

QUIZ YOURSELF

MSTP

1. What happens if you move a compressed file to a different hard disk?
2. What happens if you mark a folder for encryption and then create a new Notepad file in that folder?
3. Can you encrypt and compress a file at the same time?
4. What types of restrictions can you apply using disk quotas?
5. How does file compression interact with disk quotas?

DISASTER RECOVERY

Backup and Restore

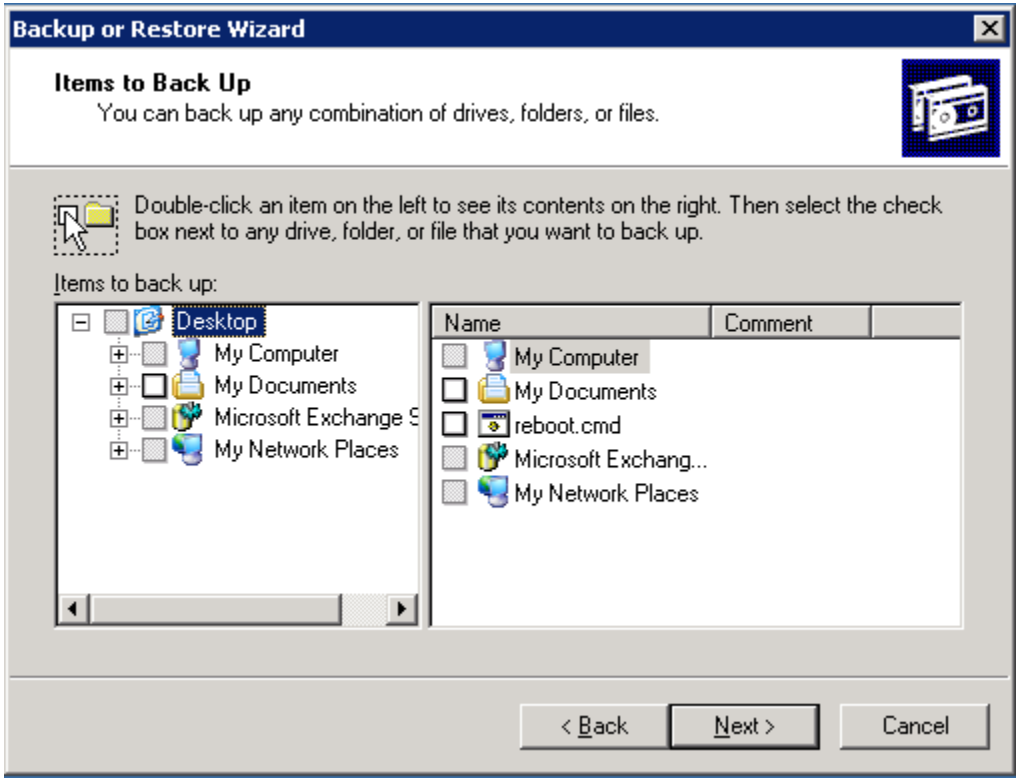
MSTP

- Windows Server 2003 includes a basic backup and restore application called Windows Backup.
  - back up the files on any computer on your network, and to back up the *system state* of the local computer to a backup file on disk or tape
- Back up the system state of computers across the network (the built-in application can back up only the local computer's system state).
- Schedule backups that include several computers across the network (while you can do this with the built-in application, it's cumbersome and time consuming).
- Manage a large set of backup media, such as tapes or optical disks.

Backing up data

MSTP

- Windows Backup enables you to back up files and the local computer's system state.
- Windows Backup can back up data either to a disk-based file or to a backup tape.



Automatic System Recovery

MSTP

- Windows Automatic System Recovery (ASR) is a last-resort process you can use to restore your server's operating system to full functionality.
  - ASR does not restore your data files, and ASR does require that you perform a special ASR backup before ASR can be used.

ASR backup

MSTP

- You use Windows Backup to perform an ASR backup. Open Windows Backup and, if you’re in Advanced mode, select ASR Wizard from the Tools menu.
- The ASR Backup Wizard automatically backs up the files required to perform an ASR restore. ASR *does not include your data files,* so make sure you perform a regular backup of those files once the ASR backup is complete.

REVIEW

MSTP

You learned about the importance of disaster recovery preparation, and you learned how to use Windows Server 2003's built-in tools for backup and restore, system snapshots, and Automatic System Recovery (ASR). You also learned how to install and log on to the Recovery console.

The greatest disadvantage to RAID 5 arrays

- available disk space is sacrificed to store the checksum information.
- total disk space equals the space available on all but one of the disks in the array
  - For example, in an array with five 10GB disks, you have a total of 40GB of available space.

File Systems

MSTP

- **FAT16.** The FAT16 file system is compatible with older operating systems like MS-DOS and Windows 95.
- **FAT32.** The FAT32 file system is more efficient than FAT16 and is compatible with Windows 98 and Windows Me (as well as later versions of Windows 95).
- **NTFS.** The NTFS file system is the best file system to use with Windows Server 2003.
  - You need to *format* the partition with the file system.
  - Formatting is a process that organizes the partition and allows the operating system to begin saving data to it

Disk Optimization

MSTP

- ***Using disks carefully***
  - Carefully planning how the disks in your computer are used can help improve disk performance.
    - use one hard drive for the operating system files and another hard drive for user data files.
  - A better solution is to use one drive for the operating system files and make a RAID 5 array from the remaining three drives.

Stripe sets for better performance

MSTP

- Windows Server 2003 supports a special type of volume called a *stripe set.*
  - stripe sets spread data across several identically sized disks
  - speeds up the process of reading data
  - stripe sets do not calculate checksum information
  - stripe sets do not provide fault tolerance
  - if one disk should fail, all of the data on the stripe set will be lost.

Disaster Recovery and Planning

MSTP

- System State
- Time Frame for the inevitable
  - Backup time
  - Restore time
- Hard Drive Redundancy
- Server Protection
  - UPS

Disaster Avoidance

MSTP

- Consider a fault tolerant disk configuration
- Multiple DC’s
- Wins replication partners
- Backup DHCP servers
- Replicated data
- Clusters for servers that need to be highly available

Restore

MSTP

- Do not use a Windows NT® 4 product
  - It will not work on new File types
  - It may fail silently
  - You will not be happy
- An exchange aware backup software is required to backup exchange properly
- Watch your backup logs and events

Disaster Recovery and Planning

MSTP

- System State
- Time Frame for the inevitable
  - Backup time
  - Restore time
- Hard Drive Redundancy
- Server Protection
  - UPS

Disaster Avoidance

MSTP

- Consider a fault tolerant disk configuration
- Multiple DC’s
- Wins replication partners
- Backup DHCP servers
- Replicated data
- Clusters for servers that need to be highly available

Additional Resources

MSTP

- Windows 2003 Help is very good and can assist with planning and best practices
- Books
- Internet
  - Google.com
    - Searches the web, technet and groups

Windows 2003 Summary

MSTP

- Multiple flavors of 2003 server
- Active directory can be designed to reflect your organization using OU's
- GPO's can help you manage your domain
  - Much like NT policy's but a lot more powerful
- Three different types of Groups in Windows 2003
- The MMC is a powerful and customizable tool
- It is a good idea to run forest prep and domain prep on the first DC in your forest if you will ever think you will be running Exchange 2003
  - This way when the new DC's come on line they will replicate all of the schema changes when they come online.

Terminal

What Is Terminal Services?

MSTP

- Terminal Services gives Windows Server 2003 the ability to act as a *terminal server.*
- A terminal server uses a centralized computing model, rather than the distributed computing model you are probably accustomed to.
- Under the covers, Terminal Services works quite differently from products like pcAnywhere.
- Most remote control products only allow a single user to control the remote computer,
- Terminal Services is designed for multiple users

Terminal Services Capabilities

MSTP

Applications can do all of the following tasks when running on a computer:

- Print documents to a print device that is attached to the computer
- Play sounds through the computer's speakers and sound card
- Access the storage devices, like hard disks and CD-ROM drives, on the computer
- Access the communications ports, such as serial ports, on the computer

When an application is running on a Terminal Services server, the application doesn't realize that it's being controlled by a user on a totally different computer.

- Documents print to the printer attached to the Terminal Services server, rather than to a printer that is physically close to the user.
- Sounds play on the server, not on the user's computer.
- Only the server's storage devices are accessible, although the user's documents might be on his computer instead of on the server.
- Only the server's communications ports are available, although the user might have devices attached to her client computer's communications ports.
- When a user connects to a Terminal Services server, the server attempts to create printers that match the printers configured on the user's client computer.

Why Use Terminal Services?

MSTP

- Terminal Services is a great way for users to remotely work on company projects.
- running application has a full-speed local area network (LAN) connection, which can handle the data.

Remote Administration with Terminal Services

MSTP

- Windows Server 2003 automatically installs Terminal Services in Remote Administration mode
  - Remote Administration mode enables members of the server's Administrators group to remotely control the server, just as if they were standing in front of it.
    - Up to two administrators can connect at once.

SCM

About the SCM

MSTP

- The SCM is designed to analyze a computer and check its compliance with a given security template, apply a security template to a computer, or create a new security template based on a computer's policy settings.
- The SCM also includes a command-line utility, **Secedit.exe**,

Security Templates

MSTP

- Security templates enable you to create standardized security policies for your computers, and then easily apply those settings to a group of computers, either using “Security Configuration and Analysis,” **Secedit.exe**, or group policies. Microsoft provides several predefined security templates, and you can modify these or create your own.

- See next slide:

Define Templates

MSTP

Policies in a template can be defined or undefined:

- When a policy is defined in the template, the policy's value overwrites a computer's local policy setting when the template is applied to that computer.
- When a policy is undefined in the template, a computer's local policy setting remains in effect when the template is applied to that computer.

Security Configuration and Analysis

MSTP

- **Import security templates.** You must import at least one security template into the analysis database.
- **Clear database prior to import.** When you import a template, you can tell Security Configuration and Analysis to clear its database prior to the import.
- **Analyze your system.** Security Configuration and Analysis compares your computer’s policy settings to the ones currently in the analysis database.

Note the icons next to each policy.

MSTP

These icons indicate whether or not the policy, as defined in the database, is active on your computer. The icons are as follows:

- A red “X” indicates that the policy values on your computer do not match those in the database.
- A green checkmark indicates that the policy values on your computer match the ones in the database.
- A **question mark** indicates that the policy is not defined in the database and was therefore not analyzed.
- An **exclamation point** indicates that the policy exists in the database and does not exist on your computer.
- **Edit the database.** You can double-click any of the policy settings in the database to change their values. Your edits affect only the database, not the policies on your computer.
- **Configure your system.** This task applies the values in the analysis database to your computer’s local policies. To perform this task, right-click Security Configuration and Analysis and select Configure Computer Now from the pop-up menu.

Secedit.exe

MSTP

- **Secedit /analyze** performs an analysis. You must specify an existing security database file using the **/db** parameter—for example, **Secedit /analyze /db mysec.sdb.**
- **Secedit /configure** configures your computer with a security template. You must specify a security database using the **/db** parameter.
- **Secedit /export** exports the security settings on your computer into a template file. You must specify the output filename.
- **Secedit /validate** compares your computer to an existing template and reports on any differences.

REVIEW

MSTP

You learned how the Security Configuration Manager (SCM) consists of several tools that can help you manage computers' security policies and other security settings. The Security Templates snap-in enables you to modify and create security templates, which can be applied to computers. Security Configuration and Analysis enables you to view templates' settings and view the result of multiple overlapping templates. Security Configuration and Analysis also enables you to apply a set of templates to your computer. **Secedit.exe** duplicates most of Security Configuration and Analysis' key functionality but works from a command line, enabling you to perform analysis and configuration tasks from batch files.